Configuring Policing

This chapter contains the following sections:

About Policing

Policing is the monitoring of the data rates for a particular class of traffic. When the data rate exceeds user-configured values, marking or dropping of packets occurs immediately. Policing does not buffer the traffic; therefore, the transmission delay is not affected. When traffic exceeds the data rate, you instruct the system to either drop the packets or mark QoS fields in them.

You can define single-rate and dual-rate policers.

Single-rate policers monitor the committed information rate (CIR) of traffic. Dual-rate policers monitor both CIR and peak information rate (PIR) of traffic. In addition, the system monitors associated burst sizes. Three colors, or conditions, are determined by the policer for each packet depending on the data rate parameters supplied: conform (green), exceed (yellow), or violate (red).

You can configure only one action for each condition. For example, you might police for traffic in a class to conform to the data rate of 256000 bits per second, with up to 200 millisecond bursts. The system would apply the conform action to traffic that falls within this rate, and it would apply the violate action to traffic that exceeds this rate.

For more information about policers, see RFC 2697 and RFC 2698.

Licensing Requirements for Policing

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco NX-OS	The QoS feature does not a require license. Any feature not included in a license package is bundled with the NX-OS image and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Prerequisites for Policing

Policing has the following prerequisites:

- You must be familiar with using modular QoS CLI.

- You are logged on to the device.

Guidelines and Limitations

Policing has the following configuration guidelines and limitations:

- Ingress and egress policing is supported on the Cisco Nexus 3100 Series platforms.

- Ingress policing is supported on the Cisco Nexus 3000 platforms.

- Egress policing is not supported on Cisco Nexus 3000 Series platforms.

- N3K-C34180YC does not support:

    - Egress policing.

    - Policing in L3 heavy mode.

    - qos qos-policies statistics.

- Each module polices independently, which might affect QoS features that are being applied to traffic that is distributed across more than one module. Policers are applied to portchannel interfaces, however policers are not supported on sub-interfaces and VLANs

- All policers in the ingress direction must use the same mode.

- The **set qos-group** command can only be used in ingress policies.

- When egress RACL and egress QoS are applied together, statistics can only be enabled for one or the other, not both.

- Egress QoS policies on ALE uplink ports on top-of-rack (TOR) platforms is not supported.

- When using egress QoS, it is recommended to use appropriate match criteria to exclusively match data traffic. (Avoid match criteria like **permit ip any any**.)

Configuring Policing

You can configure a single or dual-rate policer.

Configuring 1-Rate and 2-Rate, 2-Color and 3-Color Policing

The type of policer created by the device is based on a combination of the **police** command arguments described in the following Arguments to the police Command table.

> **Note** You must specify the identical value for **pir** and **cir** to configure 1-rate 3-color policing.

> **Note** A 1-rate 2-color policer with the violate markdown action is not supported.

> **Note** If the same policer enabled QoS policy is applied across multiple ingress interfaces on Cisco Nexus 3000 Series switches, the **qos qos-policies statistics** command should be enabled. Otherwise, the policer entry is shared between the interfaces that results in aggregate policing. The command, **qos qos-policies statistics** enables separate policer entries for each ingress interface and also enables policer statistics.

Table 1: Arguments to the police Command

Argument	Description
cir	Committed information rate, or desired bandwidth, specified as a bit rate or a percentage of the link rate. Although a value for cir is required, the argument itself is optional. The range of values is from 1 to 80000000000. The range of policing values is from 8000 to 80 Gbps.
percent	Rate as a percentage of the interface rate. The range of values is from 1 to 100 percent.
bc	Indication of how much the cir can be exceeded, either as a bit rate or an amount of time at cir. The default is 200 milliseconds of traffic at the configured rate. The default data rate units are bytes.
pir	Peak information rate, specified as a PIR bit rate or a percentage of the link rate. There is no default. The range of values is from 1 to 80000000000; the range of policing values is from 8000 bps to 480 Gbps. The range of percentage values is from 1 to 100 percent.
be	Indication of how much the pir can be exceeded, either as a bit rate or an amount of time at pir. When the bc value is not specified, the default is 200 milliseconds of traffic at the configured rate. The default data rate units are bytes. **Note** You must specify a value for pir before the device displays this argument.

Argument	Description
conform	Single action to take if the traffic data rate is within bounds. The basic actions are transmit or one of the set commands listed in the following Policer Actions for Conform table. The default is transmit.
exceed	Single action to take if the traffic data rate is exceeded. The basic actions are drop or markdown. The default is drop.
violate	Single action to take if the traffic data rate violates the configured rate values. The basic actions are drop or markdown. The default is drop.

Although all the arguments in the above Arguments to the police Command table are optional, you must specify a value for **cir**. In this section, **cir** indicates its value but not necessarily the keyword itself. The combination of these arguments and the resulting policer types and actions are shown in the following Policer Types and Actions from Police Arguments Present table.

Table 2: Policer Types and Actions from Police Arguments Present

Police Arguments Present	Policer Type	Policer Action
cir, but not **pir**, **be**, or **violate**	1-rate, 2-color	<= **cir**, **conform**; else **violate**
cir and **pir**	2-rate, 3-color	<= **cir**, conform; <= **pir**, exceed; else **violate**

The policer actions that you can specify are described in the following Policer Actions for Exceed or Violate table and the following Policer Actions for Conform table.

Table 3: Policer Actions for Exceed or Violate

Action	Description
drop	Drops the packet. This action is available only when the packet exceeds or violates the parameters.
set-cos-transmit	Sets CoS and transmits the packet.
set-dscp-transmit	Sets DSCP and transmits the packet.
set-prec-transmit	Sets precedence and transmits the packet.
set-qos-transmit	Sets qos-group and transmits the packet.

Table 4: Policer Actions for Conform

Action	Description
transmit	Transmits the packet. This action is available only when the packet conforms to the parameters.
set-prec-transmit	Sets the IP precedence field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.

Action	Description
set-dscp-transmit	Sets the differentiated service code point (DSCP) field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-cos-transmit	Sets the class of service (CoS) field to a specified value and transmits the packet. This action is available only when the packet conforms to the parameters.
set-qos-transmit	Sets the QoS group internal label to a specified value and transmits the packet. This action can be used only in input policies and is available only when the packet conforms to the parameters.

Note The policer can only drop or mark down packets that exceed or violate the specified parameters. For information on marking down packets, see the Configuring Marking section.

The data rates used in the **police** command are described in the following Data Rates for the police Command table.

Table 5: Data Rates for the police Command

Rate	Description
bps	Bits per second (default)
kbps	1,000 bits per seconds
mbps	1,000,000 bits per second
gbps	1,000,000,000 bits per second

Burst sizes used in the **police** command are described in the following Burst Sizes for the police Command table.

Table 6: Burst Sizes for the police Command

Speed	Description
bytes	bytes
kbytes	1,000 bytes
mbytes	1,000,000 bytes
ms	milliseconds
us	microseconds

.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map** [**type qos**] [**match-first**] [*policy-map-name*]
3. **class** [**type qos**] {*class-map-name* | **class-default**} [**insert-before** *before-class-name*]
4. **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [**bc** *committed-burst-rate* [*link-speed*]][**pir**] {*peak-rate* [*data-rate*] | **percent** *cir-link-percent*} [**be** *peak-burst-rate* [*link-speed*]] [**conform** {**transmit** | **set-prec-transmit** | **set-dscp-transmit** | **set-cos-transmit** | **set-qos-transmit**} [**exceed** {**drop**} [**violate** {**drop**}]]}
5. **exit**
6. **exit**
7. **show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**]
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	**Purpose**

Step 1	**configure terminal**
	
	Example:
	
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**policy-map** [**type qos**] [**match-first**] [*policy-map-name*]
	
	Example:
	
	`switch(config)# policy-map policy1`
	`switch(config-pmap-qos)#`
		Creates or accesses the policy map named *policy-map-name* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.

Step 3	**class** [**type qos**] {*class-map-name*	**class-default**} [**insert-before** *before-class-name*]
		
		Example:
		
		`switch(config-pmap-qos)# class class-default`
		`switch(config-pmap-c-qos)#`
			Creates a reference to *class-map-name* and enters policy-map class configuration mode. The class is added to the end of the policy map unless **insert-before** is used to specify the class to insert before. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.

Step 4	**police** [**cir**] {*committed-rate* [*data-rate*]	**percent** *cir-link-percent*} [**bc** *committed-burst-rate* [*link-speed*]][**pir**] {*peak-rate* [*data-rate*]	**percent** *cir-link-percent*} [**be** *peak-burst-rate* [*link-speed*]] [**conform** {**transmit**	**set-prec-transmit**	**set-dscp-transmit**	**set-cos-transmit**	**set-qos-transmit**} [**exceed** {**drop**} [**violate** {**drop**}]]}	Polices **cir** in bits or as a percentage of the link rate. The **conform** action is taken if the data rate is <= cir. If **be** and **pir** are not specified, all other traffic takes the **violate** action. If **be** or **violate** are specified, the **exceed** action is taken if the data rate <= **pir**, and the **violate** action is taken otherwise. The actions are described in the Policer Actions for Exceed or Violate table and the Policer Actions for Conform table. The data rates and link speeds are described in the Data Rates for the police Command table and the Burst Sizes for the police Command table.

Step 5	**exit**
	
	Example:
	
	`switch(config-pmap-c-qos)# exit`
	`switch(config-pmap-qos)#`
		Exits policy-map class configuration mode and enters policy-map mode.

	Command or Action	Purpose

Step 6	**exit**
	
	Example:
	`switch(config-pmap-qos)# exit`
	`switch(config)#`
		Exits policy-map mode and enters global configuration mode.

Step 7	**show policy-map** [**type qos**] [*policy-map-name* | **qos-dynamic**] **Example:** `switch(config)# show policy-map`	(Optional) Displays information about all configured policy maps or a selected policy map of type qos.

Step 8	**copy running-config startup-config**
	
	Example:
	`switch(config)# copy running-config`
	`startup-config`
		(Optional) Saves the running configuration to the startup configuration.

Example

This example shows how to display the policy1 policy-map configuration:

```
switch# show policy-map policy1
```

Configuring Ingress and Egress Policing

You can apply the policing instructions in a QoS policy map to ingress or egress packets by attaching that QoS policy map to an interface. To select ingress or egress, you specify the **input** keyword or the **output** keyword in the **service-policy** command. For more information on attaching and detaching a QoS policy action from an interface, see the Using Modular QoS CLI. section.

For egress QoS purposes, TCAM regions can be specified with the **hardware access-list tcam region** [**e-qos** \| **e-qos-lite** \| **e-ipv6-qos** \| **e-mac-qos**] *tcam-size* command.

Note All TCAM regions for egress QoS purposes are double wide, however the e-qos-lite region is single wide

Notes for Egress QoS and TCAM Regions

- Only violated and non-violated statistics are supported for policing action when the double width TCAM is used.

- Only non-violated statistics are supported for policing action when the single width TCAM (e-qos-lite) is used.

- Statistics are disabled when the optional **no-stats** keyword is used and policies are shared (where applicable).

- The **set qos-group** command is not supported for egress QoS policies.

Configuring Markdown Policing

Markdown policing is the setting of a QoS field in a packet when traffic exceeds or violates the policed data rates. You can configure markdown policing by using the set commands for policing action described in the Policer Actions for Exceed or Violate table and the Policer Actions for Conform table.

> **Note** You must specify the identical value for **pir** and **cir** to configure 1-rate 3-color policing.

SUMMARY STEPS

1. **configure terminal**
2. **policy-map** [**type qos**] [**match-first**] [*policy-map-name*]
3. **class** [**type qos**] {*class-name* | **class-default**} [**insert-before** *before-class-name*]
4. **police** [**cir**] {*committed-rate* [*data-rate*] | **percent** *cir-link-percent*} [[**bc** | **burst**] *burst-rate* [*link-speed*]] [[**be** | **peak-burst**] *peak-burst-rate* [*link-speed*]] [**conform** *conform-action* [**exceed** [**violate drop set dscp dscp table** *pir-markdown-map*]]]}
5. **exit**
6. **exit**
7. **show policy-map** [**type qos**] [*policy-map-name*]
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	**Purpose**

Step 1	**configure terminal**
	
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**policy-map** [**type qos**] [**match-first**] [*policy-map-name*]
	
	Example:
	`switch(config)# policy-map policy1`
	`switch(config-pmap-qos)#`
		Creates or accesses the policy map named *policy-map-name* and then enters policy-map mode. The policy-map name can contain alphabetic, hyphen, or underscore characters, is case sensitive, and can be up to 40 characters.

Step 3	**class** [**type qos**] {*class-name*	**class-default**} [**insert-before** *before-class-name*]
		
		Example:
		`switch(config-pmap-qos)# class class-default`
		`switch(config-pmap-c-qos)#`
			Creates a reference to *class-name* and enters policy-map class configuration mode. The class is added to the end of the policy map unless **insert-before** is used to specify the class to insert before. Use the **class-default** keyword to select all traffic that is not currently matched by classes in the policy map.

Step 4	**police** [**cir**] {*committed-rate* [*data-rate*]	**percent** *cir-link-percent*} [[**bc**	**burst**] *burst-rate* [*link-speed*]] [[**be**	**peak-burst**] *peak-burst-rate* [*link-speed*]] [**conform** *conform-action* [**exceed** [**violate drop set dscp dscp table** *pir-markdown-map*]]]}	Polices **cir** in bits or as a percentage of the link rate. The **conform** action is taken if the data rate is <= cir. If **be** and **pir** are not specified, all other traffic takes the **violate** action. If **be** or **violate** are specified, the **exceed** action is taken if the data rate <= **pir**, and the **violate** action is taken otherwise. The actions are described in the Policer Actions

	Command or Action	Purpose
		for Exceed or Violate table and the Policer Actions for Conform table. The data rates and link speeds are described in the Data Rates for the police Command table and the Burst Sizes for the police Command table.

Step 5	**exit**
	
	Example:
	`switch(config-pmap-c-qos)# exit`
	`switch(config-pmap-qos)#`
		Exits policy-map class configuration mode and enters policy-map mode.

Step 6	**exit**
	
	Example:
	`switch(config-pmap-qos)# exit`
	`switch(config)#`
		Exits policy-map mode and enters global configuration mode.

Step 7	**show policy-map** [**type qos**] [*policy-map-name*] **Example:** `switch(config)# show policy-map`	(Optional) Displays information about all configured policy maps or a selected policy map of type qos.

Step 8	**copy running-config startup-config**
	
	Example:
	`switch(config)# copy running-config`
	`startup-config`
		(Optional) Saves the running configuration to the startup configuration.

Verifying the Policing Configuration

To display the policing configuration information, perform one of the following tasks:

Command	Purpose
show policy-map	Displays information about policy maps and policing.

Configuration Examples for Policing

The following example shows how to configure policing for a 1-rate, 2-color policer:

```
configure terminal
  policy-map policy1
    class one_rate_2_color_policer
      police cir 256000 conform transmit violate drop
```

The following example shows how to configure policing for a 1-rate, 2-color policer with DSCP markdown:

```
configure terminal
  policy-map policy2
    class one_rate_2_color_policer_with_dscp_markdown
      police cir 256000 conform transmit violate set-dscp-transmit 10
```